

REMARKS

Upon entry of this amendment, claims 23, 24 and 26-34 are all of the claims pending in the application. Claims 1-22 and 35-41 have been canceled by this amendment, and claim 23 has been rewritten in independent form including all of the limitations of base claim 1. Applicants acknowledge that claims 26-28, 30 and 31 have been withdrawn from consideration.

Accordingly, because the present amendment merely involves the cancellation of claims and the rewriting of dependent claim 23 into independent form, Applicants submit that this amendment does not raise any issues that would require further consideration and/or search. As such, the present amendment should be entered.

I. Rejections under 35 U.S.C. §103(a)

A. Claims 1-3, 7, 10, 21, 22, 35, 38, and 39 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Yamada (US 2003/0135748) in view of McLean (US 5,282,247).

As noted above, claims 1-3, 7, 10, 21, 22, 35, 38, and 39 have been canceled by this amendment.

B. Claims 11-14 and 18 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Yamada (US 2003/0135748) in view of McLean (US 5,282,247) and further in view of Menezes (Handbook of Applied Cryptography, CRC Press, 1996).

As noted above, claims 11-14 and 18 have been canceled by this amendment.

C. Claims 23, 24, 29, 32-34, 36, 37, 40, and 41 have been under 35 U.S.C. § 103(a) as being unpatentable over Yamada (US 2003/0135748) in view of McLean (US 5,282,247) and further in view of Fransdonk (US 2003/0167392).

Initially, regarding claim 23, Applicants note that this claim has been rewritten in independent form so as to include all of the features of base claim 1.

Claim 23 recites that the access condition management server manages, in one-to-one correspondence, (i) identification information pieces that respectively identify a plurality of record carriers including the record carrier, and (ii) a plurality of access conditions including the access condition; and the acquisition unit (i) transmits one of the identification information pieces that identifies the record carrier to the access condition management server, and (ii) acquires the access condition corresponding to the one of the identification information pieces from the access condition management server.

The Examiner has recognized that neither Yamada nor McLean discloses the above-noted features recited in claim 23. The Examiner, however, has taken the position that Fransdonk cures this deficiency of Yamada and McLean (See Office Action at pages 13-14). Applicants respectfully disagree, and kindly request that the Examiner reconsider the rejection in view of the following comments.

Regarding Fransdonk, Applicants note that this reference discloses a condition access agent 28 that evaluates a content request from a content destination 22 based on access criteria and user credentials (see paragraph [0059]). In this regard, as explained in Fransdonk, a conditional access client 48 initiates a secure session with the conditional access agent 28 to request an order for a desired content item, whereby the conditional access client 48 parses the

request, displays order information to the user and prompts the user to enter a Personal Identification Number (PIN) code (see paragraph [0083]).

As further disclosed in Fransdonk, after receiving the display order information and the request to enter a PIN code, the user confirms the order, and the conditional access client 48 digitally signs the order confirmation using the secure device 46 (see paragraph [0083]). The signed order is then sent to the conditional access agent 28, and the conditional access agent 28 verifies the signed confirmation order and the user credentials (see paragraph [0083]).

Thus, in Fransdonk, a user requests access to content by sending a request to the conditional access agent 28. Upon receiving order information and a prompt for a PIN code from the conditional access agent 28, the user enters their PIN code and confirms the order, whereby the conditional access agent 28 then verifies the signed confirmation order and the user credentials.

As noted above, claim 23 recites that the access condition management server manages, in one-to-one correspondence, (i) identification information pieces that respectively identify a plurality of record carriers including the record carrier, and (ii) a plurality of access conditions including the access condition; and the acquisition unit (i) transmits one of the identification information pieces that identifies the record carrier to the access condition management server, and (ii) acquires the access condition corresponding to the one of the identification information pieces from the access condition management server.

In the Office Action, the Examiner has taken the position that the above-noted features recited in claim 23 are disclosed in the above-described paragraphs of Fransdonk (i.e., paragraphs [0059] and [0083]).

For example, in item 4 on pages 2-3 of the Office Action, the Examiner has stated that “Fransdonk teaches that when the user makes a request it includes its credentials and that the access agent evaluates the credential before providing access (paragraph 83)”. In addition, in item 30 on page 14 of the Office Action, the Examiner has stated that “Fransdonk discloses ... that the agent verifies the request using the user’s credentials (paragraph 83)”.

Thus, in view of the above-noted comments in the Office Action directed to the conditional access agent 28 of Fransdonk having the ability to verify a user’s credentials before providing access to a requested piece of content, the Examiner appears to be taking the position that the conditional access agent 28 in Fransdonk corresponds to the claimed “access condition management server” and that the user credentials described in Fransdonk correspond to the claimed “identification information pieces”.

With respect to such a position, however, Applicants note that claim 23 clearly indicates that the access condition management server manages identification information pieces that respectively identify a plurality of record carriers.

Accordingly, while the “identification information pieces” in Fransdonk are user credentials that respectively identify a plurality of users, Applicants note that the “identification information pieces” according to claim 23 respectively identify a plurality of record carriers.

Moreover, to the extent that the Examiner may attempt to rely on the conditional access server 36 of Fransdonk as corresponding to the claimed “access condition management server”, Applicants point out that the conditional access server 36 manages access criteria for each of a plurality of content items, not record carriers. For example, see paragraph [0083] of Fransdonk in which it is described that the “conditional access agent 28 retrieves access criteria for the requested content item”, and paragraph [0097] of Fransdonk in which it described that the

“generated access criteria are stored in a database together with the appropriate product key (optionally under a storage key), a digital signature and a content tag (i.e., a short description).”

Thus, in contrast to the conditional access server 36 of Fransdonk which manages access criteria for each of a plurality of content items, as described above, Applicants note that the access condition management server as set forth in claim 23 manages identification information pieces that respectively identify a plurality of record carriers.

In view of the foregoing, Applicants respectfully submit that while Fransdonk discloses the use of a conditional access agent 28 having the ability to verify a user's credentials, as well as a conditional access server 36 that manages access criteria for each of a plurality of content items, that that Fransdonk does not disclose or suggest the above-noted features recited in claim 23 which indicates that the access condition management server manages, in one-to-one correspondence, (i) identification information pieces that respectively identify a plurality of record carriers including the record carrier, and (ii) a plurality of access conditions including the access condition; and the acquisition unit (i) transmits one of the identification information pieces that identifies the record carrier to the access condition management server, and (ii) acquires the access condition corresponding to the one of the identification information pieces from the access condition management server.

Accordingly, Applicants submit that claim 23 is patentable over the combination of Yamada, McLean and Fransdonk, an indication of which is kindly requested.

If the Examiner maintains the above-noted rejection of claim 23, in order for Applicants to be able to make an informed decision with regard to appeal, Applicants kindly request that the Examiner explicitly identify the elements (by reference number) in Fransdonk which are being relied upon as corresponding to the claimed (i) “communication unit”, (ii) “access condition

management server”, (iii) “identification information pieces”, (iv) “plurality of record carriers”, and (v) “plurality of access conditions”.

Regarding claims 24, 29 and 32-34, as well as withdrawn claims 26-28, 30 and 31, Applicants note that these claims depend from claim 23 and are therefore considered patentable at least by virtue of their dependency.

II. Conclusion

In view of the above amendments and remarks, it is submitted that the present application is now in condition for allowance. The examiner is invited to contact the undersigned by telephone if it is felt that there are more issues remaining which must be resolved before allowance of the application.

Respectfully submitted,

Kaoru YOKOTA et al.

/Kenneth W. Fields/

By 2011.01.28 13:58:39 -05'00'

Kenneth W. Fields
Registration No. 52, 430
Attorney for Applicants

KWF/krq/asd
Washington, D.C. 20005-1503
Telephone (202) 721-8200
Facsimile (202) 721-8250
January 28, 2011